

一种改进的高性能 Lorenz 系统构造及其应用

官国荣 吴成茂 贾倩

An improved high performance Lorenz system and its application

Guan Guo-Rong Wu Cheng-Mao Jia Qian

引用信息 Citation: *Acta Physica Sinica*, 64, 020501 (2015) DOI: 10.7498/aps.64.020501

在线阅读 View online: <http://dx.doi.org/10.7498/aps.64.020501>

当期内容 View table of contents: <http://wulixb.iphy.ac.cn/CN/Y2015/V64/I2>

您可能感兴趣的其他文章

Articles you may be interested in

脉冲序列控制双断续导电模式 BIFRED 变换器的动力学建模与多周期行为

Dynamical modeling and multi-periodic behavior analysis on pulse train controlled DCM-DCM BIFRED converter

物理学报.2015, 64(1): 010501 <http://dx.doi.org/10.7498/aps.64.010501>

基于一阶广义忆阻器的文氏桥混沌振荡器研究

Wien-bridge chaotic oscillator based on first-order generalized memristor

物理学报.2014, 63(24): 240505 <http://dx.doi.org/10.7498/aps.63.240505>

非线性磁式压电振动能量采集系统建模与分析

Modeling and analysis of piezoelectric vibration energy harvesting system using permanent magnetics

物理学报.2014, 63(24): 240504 <http://dx.doi.org/10.7498/aps.63.240504>

指向 Lyapunov 指数及其在单输入单输出系统故障检测中的应用

Directional Lyapunov exponent and its application to fault detection of the single input single output system

物理学报.2014, 63(22): 220505 <http://dx.doi.org/10.7498/aps.63.220505>

电感电流伪连续模式下分数阶 Boost 变换器的非线性控制

Non-linear control for the fractional boost converter in pseudo continuous conduction mode

物理学报.2014, 63(20): 200502 <http://dx.doi.org/10.7498/aps.63.200502>

一种改进的高性能Lorenz系统构造及其应用*

官国荣^{1)†} 吴成茂¹⁾ 贾倩²⁾

1)(西安邮电大学电子工程学院, 西安 710121)

2)(陕西凌云电器集团有限公司设计所, 宝鸡 721006)

(2014年6月3日收到; 2014年8月21日收到修改稿)

Lorenz 系统是一种最具有代表性、典型性的混沌模型之一, 一直被众多学者深入研究和广泛应用. 为了获取结构和动力学行为更为复杂的混沌吸引子, 不断改善 Lorenz 系统已成为混沌动力系统研究中的重要课题之一. 为此, 本文提出了一个具有复杂系统动力学行为的改进的 Lorenz 系统, 并将其用于图像信息安全保护. 在现有各种改进的 Lorenz 系统的基础上, 首先通过增加 Lorenz 系统的控制参数和改变非线性项相结合的方法构造出一种新的 Lorenz 混沌系统; 其次采用微动力系统方法深入研究该系统并获得与 Lorenz 系统、Bao 系统、Tee 系统和 Y 系统等具有相似的耗散性、对称性、稳定性, 以及更加复杂的混沌特性和动力学行为, 同时分析该系统所产生随机序列具有良好的相关性和复杂性; 最后将其所产生的离散伪随机序列用于图像置乱和扩散加密, 通过对图像加密结果的相邻像素相关性分析、灰度空间相关特性不确定性分析、抗差分攻击以及密钥敏感性测试, 表明本文所构造的改进的 Lorenz 系统应用于图像加密能获得相对较高的安全性.

关键词: Lorenz 系统, Lyapunov 指数, 图像加密, 相关性分析

PACS: 05.45.-a, 02.30.Jr, 05.10.-a, 05.45.Tp

DOI: 10.7498/aps.64.020501

1 引言

自从1963年Lorenz发现混沌吸引子以来^[1], 混沌理论便获得了广泛的研究和应用. 随着对Lorenz系统的研究不断深入, 人们希望通过构造不同结构、不同类型的混沌系统来研究混沌演化的规律, 以求真正认识混沌现象产生的根本原因, 以便获取复杂行为的混沌系统并服务于人类. 因此, 各种改进的Lorenz混沌系统层出不穷, 并且已经在生物工程、工程力学、电力电网动态分析、社会网络系统、控制工程、经济行为、现代通信、信息安全保护等众多领域得到了广泛应用^[2-5].

针对Lorenz系统的参数不在混沌区时的不足, 1999年我国学者陈关荣教授^[6]提出了利用线性部分状态反馈控制器可以驱动非混沌的Lorenz系统出现混沌的Chen系统, 与Lorenz系统相比, Chen

系统更加复杂的动力学行为. 由于Lorenz系统和Chen系统拓扑不共轭, 无法通过拓扑变化实现两个系统的转化, 于是2002年吕金虎和陈关荣在研究两个混沌系统过程中发现了Lü系统^[7], 解决了从Lorenz系统到Chen系之间的过渡, 并构造出一个一般形式的Lorenz系统族, 将Lorenz系统、Chen系统以及Lü系统这三者之间紧密地统一起来. 2005年, 齐国元等^[8]在Lorenz系统的第一个方程式增加一个交叉乘积项, 从而获得了一种新的三维混沌系统, 该系统与之前系统不同的是具有五个平衡点、更大的Lyapunov指数和复杂的动力学行为. 随着Lorenz混沌系统的深入研究和广泛应用, 各种改进的Lorenz系统大量产生, 极大地推动了Lorenz系统理论的快速发展. 但是, 现有各种改进的Lorenz系统仍无法满足混沌通信、信息安全保护、复杂系统非线性控制等众多领域应用的需要, 于是探索混沌行为更加复杂的新系统成

* 国家自然科学基金重点项目(批准号: 61136002)、陕西省自然科学基金(批准号: 2014JM8331, 2014JQ5183, 2014JM8307)和陕西省教育厅自然科学基金专项基金(批准号: 2013JK1129)资助的课题.

† 通信作者. E-mail: guanguorong@126.com

为学者们关注的热点课题. 2002年, Elwakil等^[9]提出一种新的带有绝对值运算的Lorenz型混沌系统, 该系统可以实现两个模式混沌系统的快速切换, 能够增加系统的安全性, 且易于电路实现. 2007年, Panchev等^[10]研究了一个将Lorenz系统作为其特例的Panchev混沌系统, 该系统含有五个控制参数, 能够产生典型混沌吸引子. Zhao等^[11]通过在Lorenz系统的第一个方程增添控制项, 使原系统不混沌的条件下产生了混沌, 成功构造出一种新的改进的Lorenz系统. 王震和毛鹏伟^[12]提出类Chen系统, 能够实现在不包含经典参数的Chen系统和共轭Lorenz系统之间的转化. 2013年张转周等^[13]在原Lorenz系统模型的基础上, 通过代数方法构造出来一个具有复杂混沌吸引子的非线性混沌自治三维系统, 该系统具有Hopf分岔、复杂混沌特性的动力学行为. 2013年, Huang和Zhou^[14]通过将Lorenz系统中最后一个非线性项中的 xy 项改成 e^{xy} 得到一个含指数函数的改进的Lorenz系统, 获得了较高的Lyapunov指数, 并成功进行了电路实现. 2013年, El-Sayed和Salman^[15]提出了一种新的多参数混沌系统, 并将Lorenz系统与Chen系统统一起来, 该统一系统和Lorenz系统与Chen系统具有相同的对称性、稳定性和耗散性. 最近, 马来西亚学者Tee和Salleh^[16]通过增加原Lorenz系统控制参数, 改变原Lorenz系统第二个微分方程右端表达式, 获得了一个新的改进的Lorenz系统, 其Lyapunov指数已达到3.3549, 极大地推动了Lorenz系统的发展, 同时, 也给有效地解决当前混沌通信和数据加密等一系列热点问题带来了新的希望.

另外, 众多超混沌Lorenz系统也相继被提出, 其中2009年李春彪等^[17]将原Lorenz系统的平方项改为绝对值项, 并通过增加新的状态反馈控制器实现超混沌, 新系统具有三个平衡点和两个正的Lyapunov指数; 2013年庞寿全等^[18]在原Lorenz系统的基础上, 通过增加一个非线性控制器, 构造了一个新的四维超混沌Lorenz系统, 通过改变新引入的非线性控制器的控制参数, 可以使超混沌Lorenz系统分别呈现超混沌、混沌以及周期、拟周期等动力学行为. 这些改进的混沌系统都是通过改变原Lorenz系统模型构造出的, 大多具有结构更加复杂的动力学行为, 进一步优化和拓展了Lorenz系统.

但是, 上述这些改进的Lorenz系统及其超混

沌Lorenz系统的最大正Lyapunov指数普遍较低, 表明混沌系统运动的随机特性较弱, 特别不利于在多媒体通信、信息安全保护等领域的广泛应用. 为了获得更大的正Lyapunov指数和具有复杂结构动力学行为的混沌系统, 本文在经典Lorenz系统和三种改进Lorenz系统的基础上, 通过增加控制参数和改变非线性项的方法构造出一种新的改进的Lorenz系统, 采用微分动力系统方法研究其动力学行为特性, 新的混沌系统所产生的随机序列具有良好的自相关性和互相关性, 同时获得了相对显著增大的正Lyapunov指数和复杂度, 表明本文改进的Lorenz系统具有更为复杂的动力学行为. 为进一步研究改进系统的应用价值, 将本文改进的Lorenz混沌系统所产生的具有良好随机特性的离散序列用于图像的置乱和扩散加密, 通过对灰度图像加密结果的相关性分析、共生矩阵指标分析、差分攻击测试以及密钥敏感性等测试表明, 本文所构造的改进的Lorenz混沌映射在图像加密领域具有很大的优势, 能大大提高图像加密结果的安全性.

2 Lorenz混沌系统及其典型改进

1963年, 大气学家Lorenz给出了著名的Lorenz系统

$$\begin{cases} dx/dt = a(y - x), \\ dy/dt = bx - xz + cy, \\ dz/dt = xy - dz, \end{cases} \quad (1)$$

其中 a, b, c, d 为系统参数, 典型值为 $a = 10, b = 28, c = 1, d = 8/3$. 在保持其余参数不变, $b > 24.74$ 时, 系统进入混沌态, 最大正的正Lyapunov指数 $LE_1 = 1.2309$. 为了叙述方便, 本文将原Lorenz系统简称为原系统. 随着人们对Lorenz系统的不断深入研究, 发现Lorenz混沌序列在实现过程中存在局部单调性、序列相关性不理想和宽频带特性弱等缺陷.

在Lorenz系统发现之后的40多年里, 人们对其进行了深入的研究, 特别是陈关荣教授于1999年发现的Chen系统, 该系统吸引子具有更复杂的拓扑结构和更复杂的动力学行为, 因而更适合于混沌信息加密和混沌通信.

2002年Lü系统的诞生, 在Lorenz系统和Chen系统之间建立了一座桥梁. 同时, 在研究Lorenz系统和Chen系统类似性的基础上, Celikovskiy和

Chen^[19]引入广义Lorenz系统族,它能够统一经典的Lorenz系统、Chen系统、Lü系统以及广义Lorenz系统,作为Lorenz系统、Lü系统和Chen系统之间的光滑链接.该系统可表述为

$$\begin{cases} \frac{dx}{dt} = (25\alpha + 10)(y - x), \\ \frac{dy}{dt} = (28 - 35\alpha)x + (29\alpha - 1)y - xz, \\ \frac{dz}{dt} = -(\alpha + 8)/3z + xy, \\ \alpha \in [0, 1]. \end{cases} \quad (2)$$

这个统一系统本质上是Lorenz系统和Chen系统的凸组合,然而,它代表了由中间无穷多个混沌系统组成的整个族,而Lorenz系统和Chen系统是它的两个极端,当 $\alpha = 0$ 时,它是Lorenz系统;当 $\alpha = 1$ 时,它成为Chen系统;当 α 在0与1之间变化时,所有的系统均保持混沌状态.除此之外,还有不少学者围绕Lorenz混沌系统做了大量研究,特别是2009年Sun和Sprott^[20]提出了单参数的简化Lorenz混沌系统,其数学模型描述为

$$\begin{cases} dx/dt = 10(y - x), \\ dy/dt = -xz + (24 - 4c)x + cy, \\ dz/dt = xy - 8z/3, \end{cases} \quad (3)$$

其中 c 为系统的分岔参数,当 $c \in [-1.59, 7.75]$ 时,系统是混沌的;当 $c = -1$ 时,它是标准的Lorenz系统;当 $c = 6$ 时,该系统的第2个方程不含 x 项;当 $c = 0$ 时,该系统的第2个方程不含 y 项.所以,该系统包括了不同的拓扑结构,具有丰富的动力学特性,为混沌的理论与应用研究提供了一个新的模型.

在Lü混沌系统的基础上,包伯成等^[21,22]将第3个方程中非线性项修改为 x^2 项并得到简称为Bao系统的三维混沌,其数学模型为

$$\begin{cases} dx/dt = a(x - y), \\ dy/dt = xz - cy, \\ dz/dt = x^2 - bz, \end{cases} \quad (4)$$

当 $a = 20, b = 4, c = 32$ 时, Bao系统进入混沌状态,具有复杂的动力学行为;相应的最大Lyapunov指数为 $LE_1 = 2.8019$, Lyapunov维数为 $d_L = 2.1492$.相比较于原Lorenz混沌系统, Bao系统在代数方程结构上较为简单,具有更大的正Lyapunov指数和较为复杂的混沌吸引子.为了叙述方便,将该系统简称为Bao系统.

2013年,马来西亚学者Tee和Salleh提出了一个新的改进的Lorenz混沌系统^[16]为

$$\begin{cases} dx/dt = a(by - x), \\ dy/dt = cx - xz, \\ dz/dt = xy - bz, \end{cases} \quad (5)$$

当 $a = 10, b = 10.629, c = 20$ 时,计算Lyapunov指数分别为 $LE_1 = 3.354912, LE_2 = 0, LE_3 = -23.879563$,可以看出该模型结构简单,具有很好的混沌特性.为了叙述方便,将该系统简称为Tee系统.

2009年,袁地提出了类Lorenz混沌系统^[23],即

$$\begin{cases} dx/dt = a(y - x), \\ dy/dt = cx - xz, \\ dz/dt = x^2 - bz, \end{cases} \quad (6)$$

当 $a = 7, b = 2, c = 25$ 系统时,该系统的Lyapunov指数分别为 $LE_1 = 1.1949, LE_2 = 0, LE_3 = -10.1932$, Lyapunov维数为 $d_L = 2.1172$.该系统虽然结构简单,但是复杂度低且随机性弱.为了叙述方便,将该系统简称为Y系统.

除了上述典型改进的Lorenz系统外,最近Luo等^[24]又提出了改进的Lorenz系统,其数学模型为

$$\begin{cases} dx/dt = a(y - x), \\ dy/dt = by - xz, \\ dz/dt = g(y) - c, \end{cases} \quad (7)$$

当 $a = 2, b = 0.6, c = 0.49, g(y) = y^2$ 时,通过仿真,该系统会产生具有两个窝圈的混沌吸引子, Lyapunov指数分别为 $LE_1 = 0.1322, LE_2 = 0, LE_3 = -0.6178$,可以看出该系统的正Lyapunov指数较低.另外,将该系统中的表达式 $g(y)$ 用平方函数与符号函数相结合的 $f_N(y) = g(y) + \sum_{i=1}^N \{A_i[\text{sgn}(y + a_i) - \text{sgn}(y - a_i) - 2]\}$ 代替并获得8窝圈混沌系统;同时,将其第二个微分方程右端适当修改能获得较多窝圈的复杂混沌系统.但是,这两个改进系统的正Lyapunov指数均小于0.25.

为了实现简单非线性动力系统获取复杂动力学行为的需要,利用上述典型改进混沌系统的构造思路和方法,本文探索一种新的改进的Lorenz混沌系统.

3 一种新的改进的Lorenz混沌系统

为了构造新的混沌系统, 本文将Tee系统三个非线性方程中的 xy 改为 x^2 , 同时增加一个控制参数 d , 于是便获得如下新的系统为

$$\begin{cases} dx/dt = a(dy - x), \\ dy/dt = cx - xz, \\ dz/dt = x^2 - bz, \end{cases} \quad (8)$$

当 $a = 20, b = 9, c = 25, d = 15$ 时, 求出该系统的Lyapunov指数分别为 $LE_1 = 7.0661, LE_2 = 0.0056158, LE_3 = -36.0523$. 特别地, 当 $d = 1$ 时, 该系统退化为Y系统. 为了叙述方便, 将本文建议的改进系统(8)式简称为新系统. 通过比较分析新系统与其他典型系统的Lyapunov指数, 发现新系统具有明显增大的最大正Lyapunov指数, 其混沌行为更为复杂. 设定各混沌系统的初始值为 $(1, 1, 1)$, 利用matlab软件仿真各系统并获得其混沌吸引子相位图如图1—图5所示.

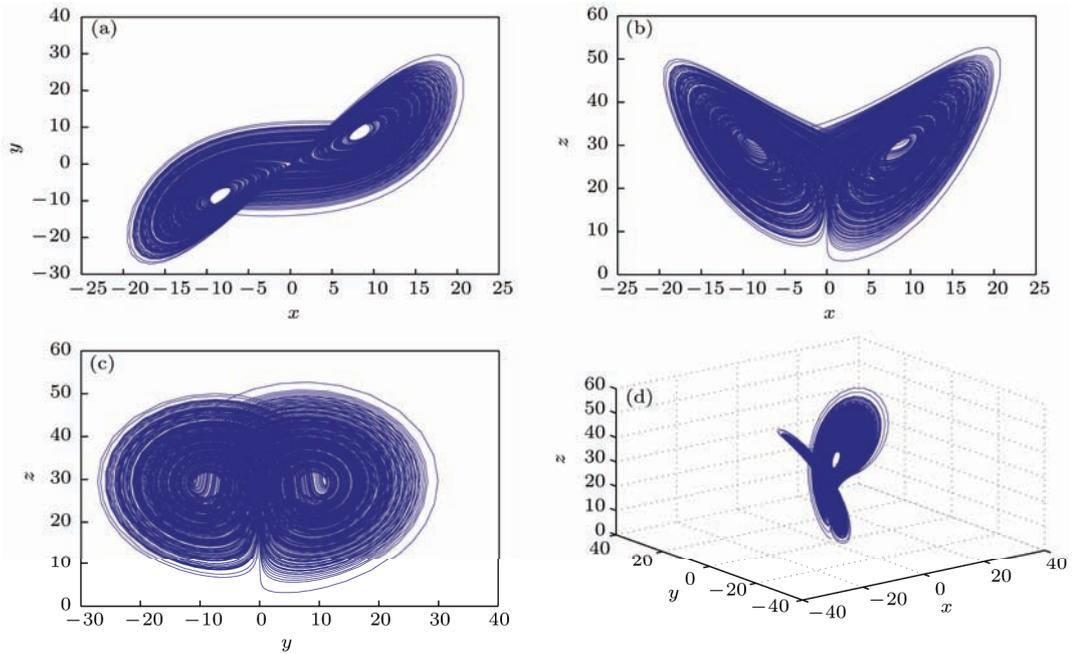


图1 在 $a = 10, b = 28, c = 1, d = 8/3$ 时原系统吸引子相图 (a) x - y 平面; (b) x - z 平面; (c) y - z 平面; (d) x - y - z

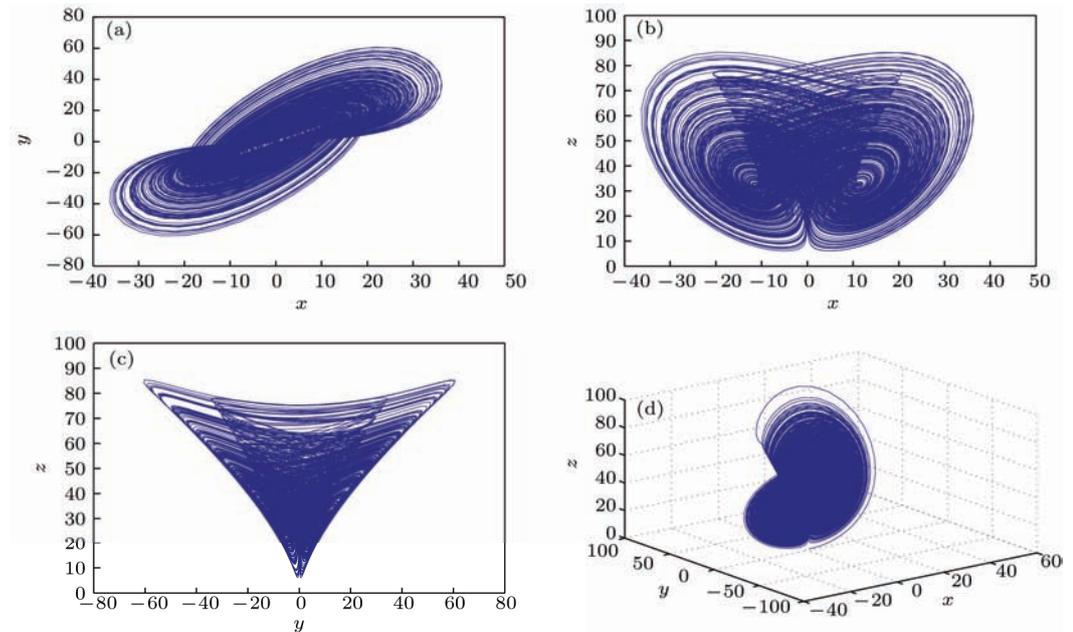


图2 在 $a = 20, b = 4, c = 32$ 时Bao系统吸引子相图 (a) x - y 平面; (b) x - z 平面; (c) y - z 平面; (d) x - y - z

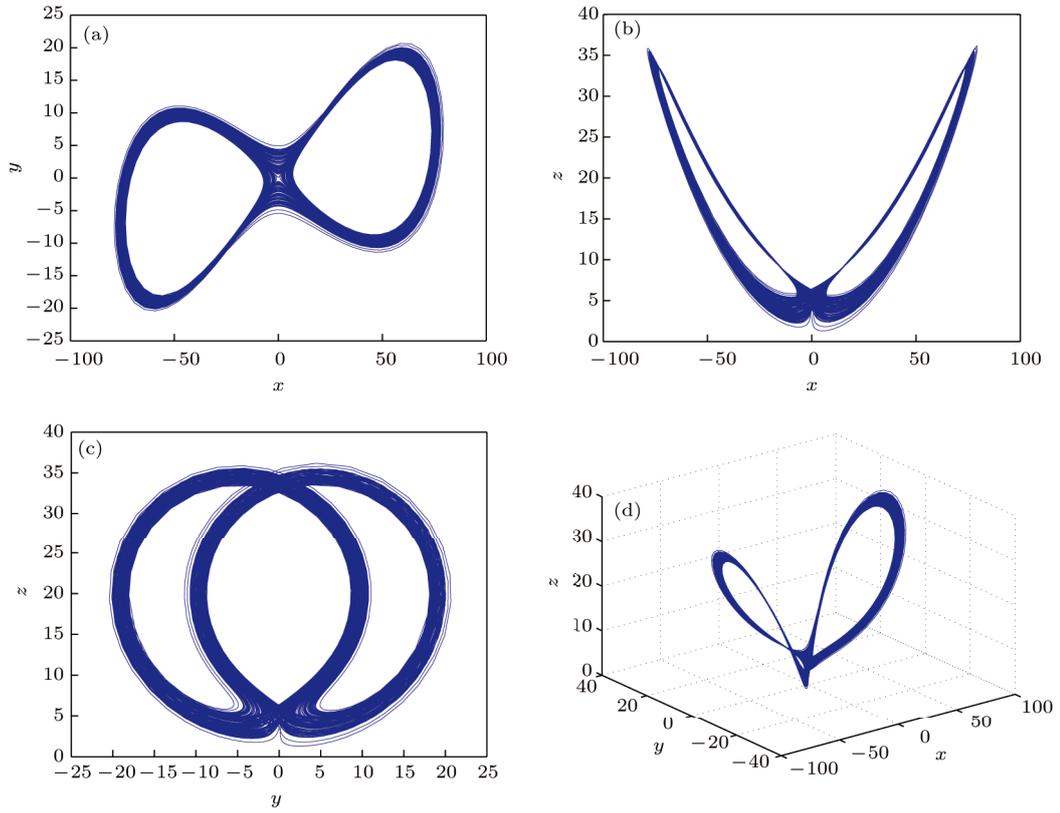


图3 在 $a = 10, b = 10.629, c = 20$ 时 Tee 吸引子相图 (a) $x-y$ 平面; (b) $x-z$ 平面; (c) $y-z$ 平面; (d) $x-y-z$

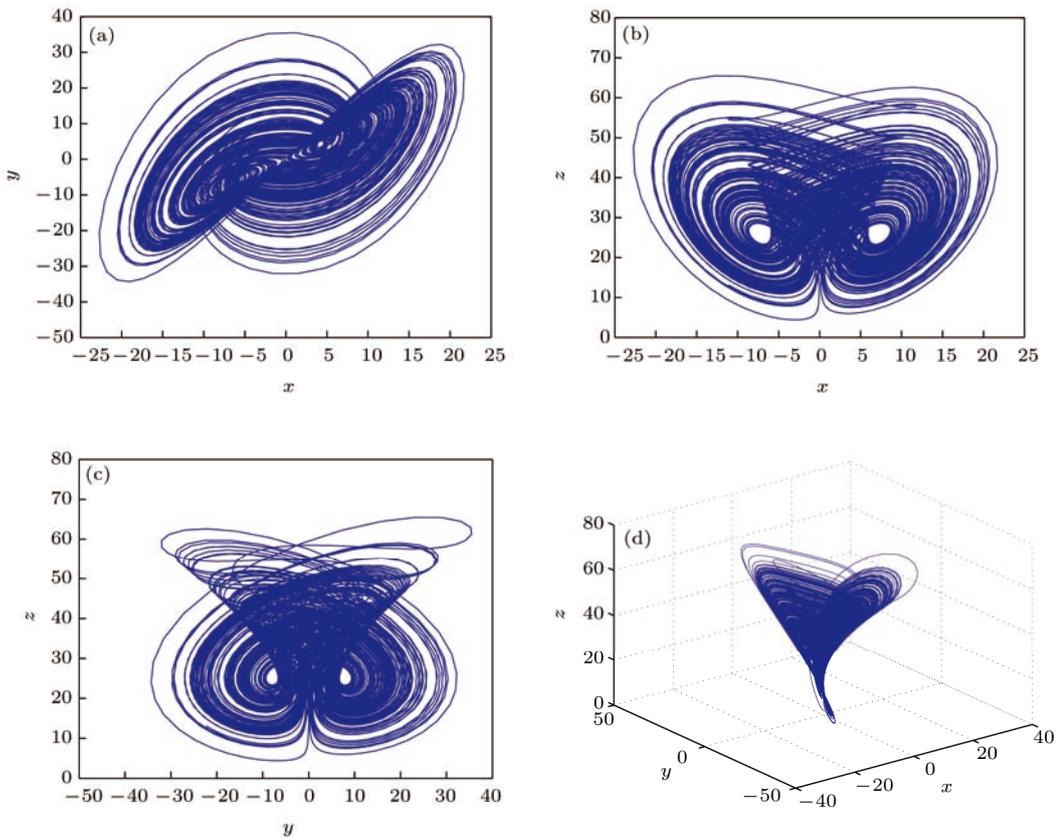


图4 在 $a = 7, b = 2, c = 25$ 时 Y 系统吸引子相图 (a) $x-y$ 平面; (b) $x-z$ 平面; (c) $y-z$ 平面; (d) $x-y-z$

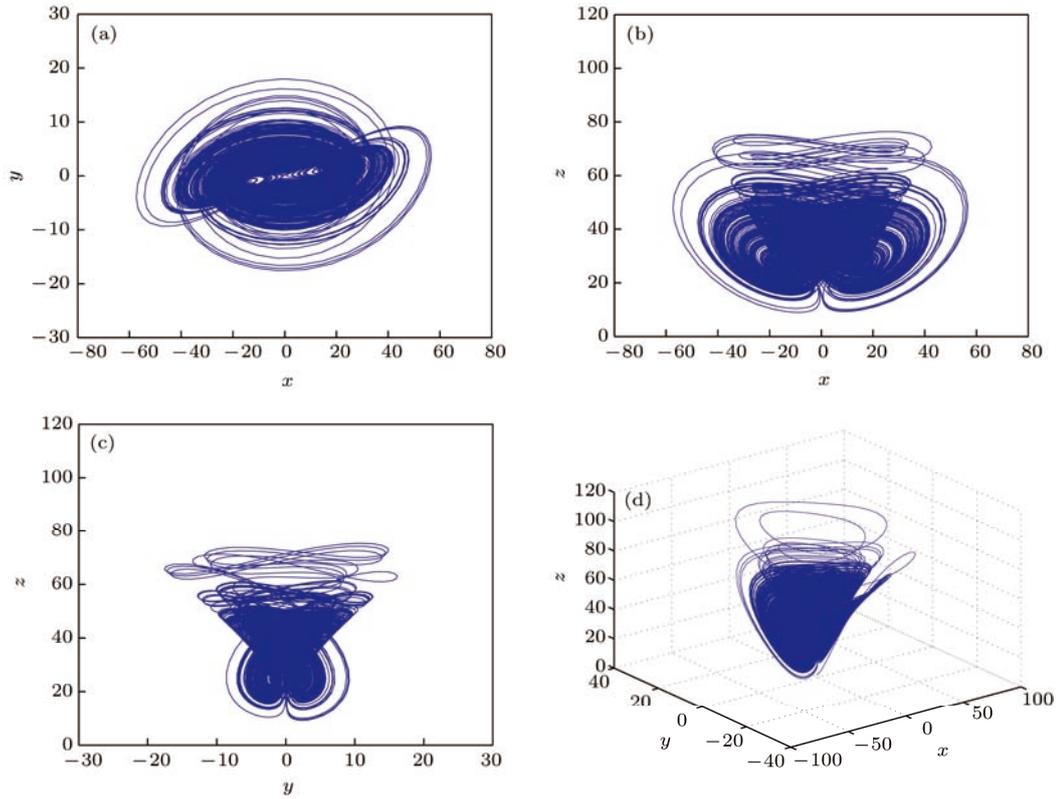


图5 在 $a = 20, b = 9, c = 25, d = 15$ 时新系统吸引子相图 (a) $x-y$ 平面; (b) $x-z$ 平面; (c) $y-z$ 平面; (d) $x-y-z$

从图1—图5所示的仿真结果来看, 本文所建议的新系统所对应的混沌吸引子有很强的吸引性, 具有复杂的折叠和拉伸轨线, 这表明该系统明显处于混沌状态.

4 新混沌系统的动力学分析

从系统动力学角度出发, 本文对新构造的混沌系统进行深入研究, 并比较了它与典型改进的Lorenz系统之间的差异性.

4.1 对称性与耗散性

针对本文所建议的新系统, 存在一个对称变换 $S : (x, y, z) \rightarrow (-x, y, z)$, 使得该系统在变换 S 的作用下明显具有不变性. 因此, 新系统关于 Z 轴对称. 通过计算新系统的耗散性, 可得到如下表达式

$$\begin{aligned} \nabla V &= \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} \\ &= a - b < 0, \end{aligned} \quad (9)$$

这就意味着当 $a + b > 0$ 时, 新系统总是耗散的; 当初始参数 $a = 20, b = 9, c = 25, d = 15$ 时, 则有

$a + b = 29$, 说明新系统在该参数条件下的状态变化是有界的, 并以指数形式 $dV/dt = e^{-29t}$ 收敛到零. 因此, 新系统运动轨线将被吸引在一个体积为零的集合上^[25].

4.2 平衡点稳定性

为了获取新系统的平衡点, 令 $dx/dt = dy/dt = dz/dt = 0$, 即有 $a(dy - x) = 0, cx - xz = 0, x^2 - bz = 0$, 于是可得到新系统的平衡点分别是 $(0, 0, 0), (\pm\sqrt{bc}, \pm\sqrt{bc}/d, c)$. 针对本文所建议的新系统, 其Jacobian矩阵为

$$J = \begin{bmatrix} a & ad & 0 \\ c & z & 0 \\ 2x & 0 & b \end{bmatrix}. \quad (10)$$

根据(10)式, 可得到特征方程为

$$\begin{aligned} \lambda^3 + (a + b)\lambda^2 + (ab + ad(z - c))\lambda \\ + 2x^2ad + abd(z - c) = 0. \end{aligned} \quad (11)$$

当 $a = 20, b = 9, c = 25, d = 15$ 时, 新系统的三个平衡点分别为: $S_1 = (0, 0, 0), S_2 = (15, 1, 25)$ 和 $S_3 = (-15, 1, 25)$. 将 $S_1 = (0, 0, 0)$ 代入(11)

式可求得三个特征根分别为 $\lambda_1 = -97.178$, $\lambda_2 = 77.178$, $\lambda_3 = -9$, 其特征根不全为正或负, 表明 $S1$ 平衡点是不稳定鞍点^[26]. 同理, 平衡点 $S2$ 和 $S3$ 所对应的线性化系统特征根分别为 $\lambda_1 = -61.6262$ 和 $\lambda_{2,3} = 16.3131 \pm 43.8692i$. 非零平衡点 $S2$ 和 $S3$ 为指数 2 的不稳定焦点, 可形成混沌吸引子的两个涡

圈. 另外, 其他四个典型混沌系统的平衡点稳定性如表 1 所示.

从表 1 所示的 5 个混沌系统的平衡点和稳定性来看, 新系统与原系统、Bao 系统、Tee 系统以及 Y 系统的平衡点具有相似的性质, 即具有一个不稳定鞍点、两个不稳焦点.

表 1 混沌系统的平衡点和稳定性

系统	初值	平衡点	特征根	
原系统	$a = 10$	$S1(0, 0, 0)$	$\lambda_1 = -25.2425$	
	$b = 40$		$\lambda_2 = 16.2425$	
	$c = 1$		$\lambda_3 = -2.5$	
	$d = 2.5$		$S2(10.12, 10.12, 41)$	$\lambda_1 = -13.4929$
		$S3(-10.12, -10.12, 41)$	$\lambda_{2,3} = 0.9965 \pm 12.2805i$	
Bao 系统	$a = 20$	$S1(0, 0, 0)$	$\lambda_1 = 20$	
	$b = 4$	$S2(8\sqrt{2}, 8\sqrt{2}, 32)$	$\lambda_2 = -4\lambda_3 = -32$	
	$c = 32$	$S3(-8\sqrt{2}, -8\sqrt{2}, 32)$	$\lambda_1 = -23.3413$	
			$\lambda_{2,3} = 3.6706 \pm 14.3485i$	
Tee 系统	$a = 10$	$S1(0, 0, 0)$	$\lambda_1 = -51.3767$	
	$b = 10.629$		$\lambda_2 = 41.3767$	
	$c = 20$		$S2(47.53, 4.47, 20)$	$\lambda_3 = -10.6290$
			$S3(-47.53, -4.47, 20)$	$\lambda_1 = -19.3061$
			$\lambda_{2,3} = -0.6615 \pm 48.3675i$	
Y 系统	$a = 7$	$S1(0, 0, 0)$	$\lambda_1 = -2$	
	$b = 2$		$\lambda_2 = -17.1839$	
	$c = 20$		$S2(7.0711, 7.0711, 25)$	$\lambda_3 = 10.1839$
			$S3(-7.0711, -7.0711, 25)$	$\lambda_1 = 6.3184$
			$\lambda_{2,3} = -7.6592 \pm 7.219i$	
新系统	$a = 20$	$S1(0, 0, 0)$	$\lambda_1 = -97.178$	
	$b = 9$		$\lambda_2 = 77.178$	
	$c = 25$			$\lambda_3 = -9$
			$S2 = (15, 1, 25)$	$\lambda_1 = -61.6262$
			$S3 = (-15, -1, 25)$	$\lambda_{2,3} = 16.3131 \pm 43.8692i$

4.3 Lyapunov 指数和维数

Lyapunov 指数是衡量系统动力学特性的一个重要定量指标^[27], 它表征了系统在相空间中相邻轨道间收敛或发散的指数率. 利用四阶 Runge-Kutta 方法数值模拟求解本文新系统的 Lyapunov 指数, 设定系统初值为 (1, 1, 1), 在 $a = 20$, $b = 9$, $c = 25$ 固定不变的情况下, 仿真随 d 变化的 Lyapunov 指数谱^[28] 和系统的分岔图如图 6(a) 和 (b) 所示, 从图 6(a) 可以看出, 当 $d \in (0, 26)$ 时, 新系统具有一个正的 Lyapunov 指数, 系统处于混沌状态; 图 6(b) 中随着 d 的增大, 系统由不动点进入一个较大的混沌区域, 在混沌带中系统存在多个周期窗口, 都具有逆、倍周期分岔现象, 分岔图和 Lyapunov 指数谱有着完全一致

的动力学行为. 同时给出当 $d = 15$ 时, 新系统的 Lyapunov 指数随时间变化的曲线如图 6(c) 所示, 此时新系统最大正 Lyapunov 指数为 7.0661.

混沌吸引子具有无穷层次的自相似结构, 可以用维数来表征它的离散程度. 相轨道的自相似结构使得其相轨线不能填满整个相空间, 从而形成了混沌系统所特有的分形结构, 具有分数维数的特征, 因此分数维数也是判断混沌运动的有效手段.

计算 Lyapunov 维数的公式为:

$$d_L = j + \frac{1}{|LE_{j+1}|} \sum_{i=1}^j LE_i,$$

由于本文研究的都是三维混沌系统, 因此这里 $j = 2$. 利用各系统的 Lyapunov 指数求出系统维数, 比较五个系统的 Lyapunov 指数和维数, 具体如

表2所示。

从表2可以看出，五个系统都具有一个正的Lyapunov指数，维数都为分数，但新系统具有相对较大的正Lyapunov指数和维数，表明本文所构造新系统具有明显的混沌优势。

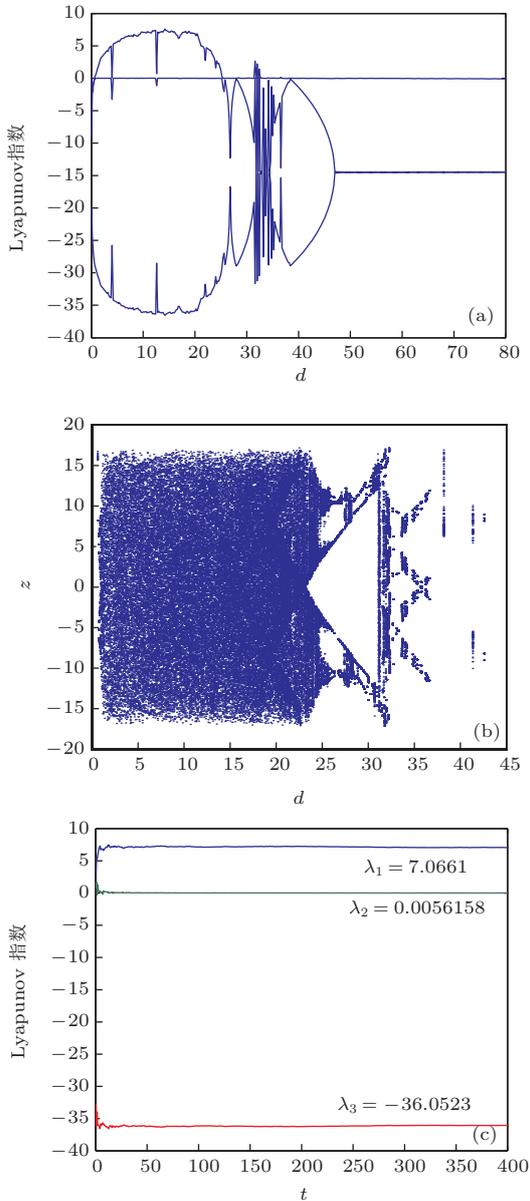


图6 新系统关于参数d的Lyapunov指数图和分岔图 (a) 随d变化的Lyapunov指数谱; (b) 随d变化的分岔图; (c) d = 15时的Lyapunov指数

4.4 混沌序列相关性分析

序列的相关性分为自相关性和互相关性，它们分别表示时间序列任意两个不同时刻取值之间，以及两个时间序列相同时刻取值之间的相关程度和混沌序列相关性的好坏，直接影响在实际应用中性

能的优劣[29,30]。

相关性分析的具体方法描述为：首先选取两个初始值 x_0 和 y_0 ，产生两不同的混沌序列 x_1 和 x_2 ，设模拟序列 x 的均值为 \bar{X} ；其次根据混沌序列自相关函数和互相关函数，即

$$\begin{cases} R_{ac}(m) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} (x_i - \bar{X}) \\ \quad \times (x_{i+m} - \bar{X}), \\ R_{cc}(m) = \lim_{x \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} (x_{1i} - \bar{X}) \\ \quad \times (x_{2(i+m)} - \bar{X}), \end{cases} \quad (12)$$

计算出新系统的混沌序列自相关和互相关性的波形，如图7所示。

表2 混沌系统的Lyapunov指数和维数

系统	初始参数	Lyapunov 指数	Lyapunov 维数
原系统	$a = 10,$	$LE_1 = 1.2132$	$d_L = 2.0955$
	$b = 40,$	$LE_2 = 0$	
	$c = 1,$	$LE_3 = -12.7082$	
	$d = 2.5$		
Bao 系统	$a = 20,$	$LE_1 = 2.8014$	$d_L = 2.1492$
	$b = 4,$	$LE_2 = 0$	
	$c = 32$	$LE_3 = -17.7719$	
Tee 系统	$a = 10,$	$LE_1 = 3.3549$	$d_L = 2.1405$
	$b = 10.629,$	$LE_2 = 0$	
	$c = 20$	$LE_3 = -23.8796$	
Y 系统	$a = 7,$	$LE_1 = 1.1949$	$d_L = 2.1172$
	$b = 2,$	$LE_2 = 0$	
	$c = 20$	$LE_3 = -10.1932$	
新系统	$a = 20,$	$LE_1 = 7.0661$	$d_L = 2.196$
	$b = 9,$	$LE_2 = 0$	
	$c = 25,$	$LE_3 = -36.0523$	
	$d = 15$		

从图7可见，新系统产生的随机序列具有良好的相关性。另外，为了更客观地比较新系统和其他系统产生随机序列相关性的差异，分别利用上述五个混沌系统所产生长度为500的随机序列，求其自相关和互相关的最大值、最小值和波动平均值，并进行比较，如表3所示，其中自相关的最大值是除去1之外的最大值。

从表3可以看出，五个混沌系统所产生随机序列都具有良好的自相关性和互相关性；但是，从自相关和互相关的最大值、最小值和波动平均值来看，本文新系统产生随机序列相关特性较为稳定，且波动更小，能满足扩频通信和图像加密等众多领域应用需要。

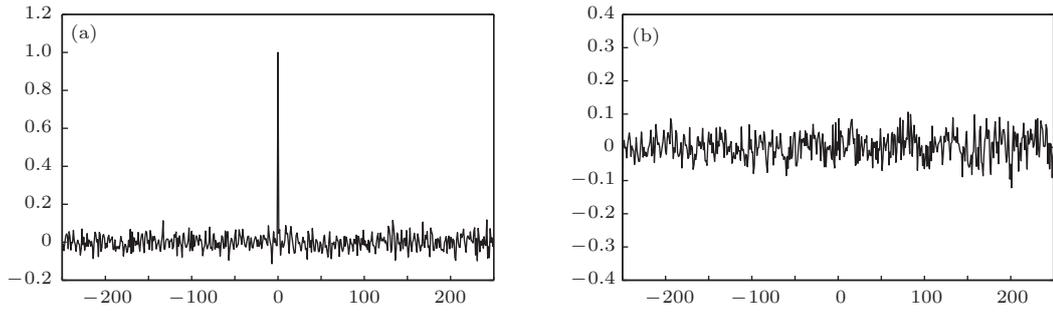


图7 新系统产生混沌序列的相关性 (a) 自相关; (b) 互相关

表3 混沌系统的自相关和互相关值

混沌系统	自相关性			互相关性		
	最大值	最小值	波动平均值	最大值	最小值	波动平均值
原系统	0.11842	-0.14211	0.03191	0.11298	-0.09524	0.02951
Bao 系统	0.11236	-0.13822	0.02967	0.11889	-0.10156	0.02994
Tee 系统	0.10102	-0.11915	0.02934	0.12623	-0.12668	0.03011
Y 系统	0.13464	-0.13263	0.03052	0.10939	-0.10084	0.03021
新系统	0.12308	-0.10783	0.02892	0.11128	-0.13324	0.02987

5 混沌系统复杂度分析

一般而言, 除常采用 Lyapunov 指数、维数来度量混沌系统的随机特性外, 学者们提出采用近似熵、模糊熵等来描述混沌轨道随时间演化信息的产生率来度量混沌序列的复杂程度^[31,32]. 计算近似熵的方法如下:

1) 给定一个长度为 N 时间序列 $L(1), L(2), \dots, L(N)$, 按顺序将其组成一个 m 维的向量集 $\mathbf{X}(i)$, 即

$$\mathbf{X}(i) = [L(i), L(i+1), \dots, L(i+m-1)],$$

$$i = 1, 2, 3, \dots, N-m+1;$$

2) 计算任意向量 $\mathbf{X}(i)$ 与其余向量 $\mathbf{X}(j)$ 之间的距离 $d[\mathbf{X}(i), \mathbf{X}(j)]$

$$d[\mathbf{X}(i), \mathbf{X}(j)] = \max |x(i+k) - x(j+k)|,$$

$$k = 0, 1, \dots, m-1, \quad (13)$$

即两向量对应元素之间差值绝对值的最大值就是两向量之间的距离;

3) 给定阈值 $r (r > 0)$, 对于每一个 i 值, 记录满足条件 $d[\mathbf{X}(i), \mathbf{X}(j)] < r$ 的个数, 把这个值与

$N-m$ 的比值定义为 $C_i^m(r)$;

4) 对每一个可能的 i 值, 计算 $C_i^m(r)$ 的自然对数, 这些对数的平均值定义为

$$\phi^m(r) = \frac{1}{N-m+1} \sum_{i=1}^{N-m+1} \ln C_i^m(r); \quad (14)$$

5) m 增加 1, 重复前面四个过程, 求得 $C_i^{m+1}(r)$ 和 $\phi^{m+1}(r)$, 求出近似熵

$$\text{ApEn} = \sum_{N \rightarrow \infty} [\phi^m(r) - \phi^{m+1}(r)], \quad (15)$$

ApEn 表示向量集随着 m 增大信息产生的概率, 产生信息的概率越大, ApEn 值就越大, 即时间序列的复杂度越大.

按照上述方法求取近似熵时, 令 $N = 2000$, $m = 2$, $r = 0.15$, 分别求出五个混沌系统所产生随机序列的复杂度计算结果列于表 4.

从表 4 所示的五个混沌系统产生随机序列所对应的近似熵值来看, 本文新系统产生混沌序列的近似熵值相对较大, 说明新系统的复杂度更高. 另外, 通过对比不同系统的 Lyapunov 指数、维数和近似熵, 都可得到相同的结论. 这些指标值表明本文新系统具有潜在的混沌优势.

表4 混沌系统产生随机序列的近似熵计算

系统	$X(1)$	$X(2)$	$X(3)$
原系统	0.4306	0.5040	0.4394
Bao 系统	0.5981	0.6258	0.6258
Tee 系统	0.3829	0.4301	0.1889
Y 系统	0.5064	0.5731	0.4552
新系统	0.6568	0.7078	0.4576

6 新系统在图像加密中的应用

将新系统产生的离散序列用于图像的置乱和扩散加密中,以便进一步验证新系统的混沌特性.

6.1 图像像素位置置乱方法

本文利用一种基于混沌序列置乱像素位置的方法,可使得置乱结果能达到抵抗选择明文攻击的目的^[33]. 设 M 和 N 分别是待加密图像的像素行数和列数,在图像置乱过程中,从混沌系统所得的3个混沌序列中随机选取2个,并从中截取长度等于行数 M 的序列 X_1 和长度等于列数 N 的序列 X_2 , 然后对序列 X_1 按从小到大的顺序排序得到 A , 并记录 A 中的每个元素在 X_1 中的位置得到 r , 同理利用序列 X_2 进行排序得到位置序列 c . 可以看出 $r = \{r_i, i = 1, 2, \dots, M\}$, $c = \{c_i, i = 1, 2, \dots, N\}$, 且 r 是 $[1, M]$ 范围的整数、 c 是 $[1, N]$ 范围的整数. 利用序列 r 和 c 对待加密图像实施行列置乱, 将待加密图像和置乱后的图像记为 P 和 P^{rc} , 通过 (16) 式来完成行列置乱:

$$P^{rc}(i, j) = P(r_i, c_j). \quad (16)$$

从 (16) 式中可以看出来, 置乱后的图像 P^{rc} 的第 i 行就是原图像 P 的第 r_i 行, P^{rc} 的第 j 列就是原图像行置乱后的第 c_j 列.

6.2 图像像素值加密方法

在完成图像行列位置置乱之后, 利用混沌系统产生的混沌序列对置乱后图像的像素值进行替代^[34]. 首先, 利用混沌系统产生的3个长度为 $M \times N/3$ 混沌序列, 并进行如下离散化处理:

$$H_i = \text{mod}((|x_i| - \text{floor}(|x_i|)) \times 10^{14}, 256) \quad i = 1, 2, 3 \quad (17)$$

(17) 式将混沌序列改造成 $[0, 255]$ 范围的整数序列, 将这三个整数序按顺序连接成为一个长度为

$M \times N$ 的整数密钥序列 B , 即 $B = \{H_1, H_2, H_3\}$. 利用 B 对 P^{rc} 进行像素变换, 其变化原则是:

$$C_j = P_j^{rc} \oplus \{\text{mod}[(B_j \oplus C_{j-1}), 256]\} \quad j = 1, 2, \dots, M \times N, \quad (18)$$

(18) 式中 B_j 就是由前述三个离散化混沌序列连接组成的总混沌密钥序列; 置乱图像的像素序列为 P_j^{rc} , 最终加密图像的像素序列为 C_j , 第一个像素点 C_0 是一个指定常数. 接下来按照上述方法对图像进行加密.

6.3 灰度图像加密测试

利用新系统产生的混沌序列对图像进行加密, 限于篇幅有限, 本文仅对 256×256 的 Lena 灰度图像进行仿真测试, 其结果如图 8 所示.

从图 8 (a) 和 (c) 所示的原始图像、置乱图像来看, 置乱后的图像像素点位置发生了很大的变化, 但只是破坏相邻像素的相关性, 没有改变图像像素值, 如果获取整数列 r 和 c , 那么就很容易破译, 为此须对置乱图像的像素值进行改变.

从图 8 (a), (d) 和 (e) 所示的原始图像、加密图像以及其直方图来看, 加密后原始图像的像素点位置和大小都发生了改变, 同时灰度统计直方图特性发生巨大变化, 其加密结果能够抵抗统计攻击.

6.4 加密图像相关性分析

相邻像素的相关性和统计特性是评价图像加密效果的重要指标, 为此, 本文通过对比加密前后图像相邻像素的分布图, 相关系数及其统计特性, 以便研究不同混沌系统的加密效果. 利用 matlab 软件, 仿真测试新系统产生随机序列置乱加密灰度 Lena 图像, 其加密前后不同方向相邻像素任取 1000 对的分布图如图 9 和图 10 所示.

从图 9 和图 10 所示的原图像和加密图像的相邻像素分布来看, 加密后图像的像素分布更加分散和均匀, 加密效果明显. 为了进一步评价图像加密像素空间分布特性, 可利用相邻像素联合共生二维直方图^[35]所对应的信息熵定量刻画相邻像素空间分布均匀程度大小. 限于篇幅, 仅给出新系统加密图像 4 个不同方向相邻像素共生二维直方图, 如图 11 所示. 为了更清楚地了解加密图像相邻像素空间分布均匀程度, 不同系统加密图像所对应的不同方向相邻像素的二维统计直方图熵和相关系数的对比如表 5 所示.

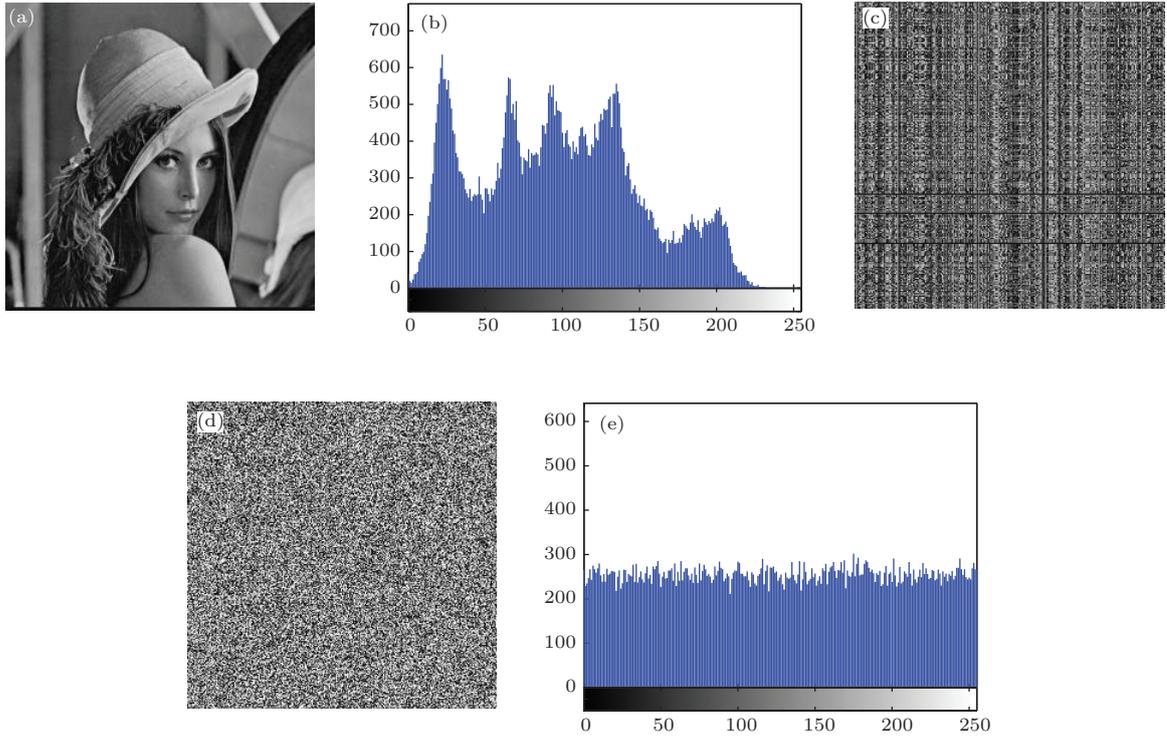


图8 利用新系统产生混沌序列进行图像加密 (a) 原始图像; (b) 原始图像直方图; (c) 置乱图像; (d) 加密图像; (e) 加密图像直方图

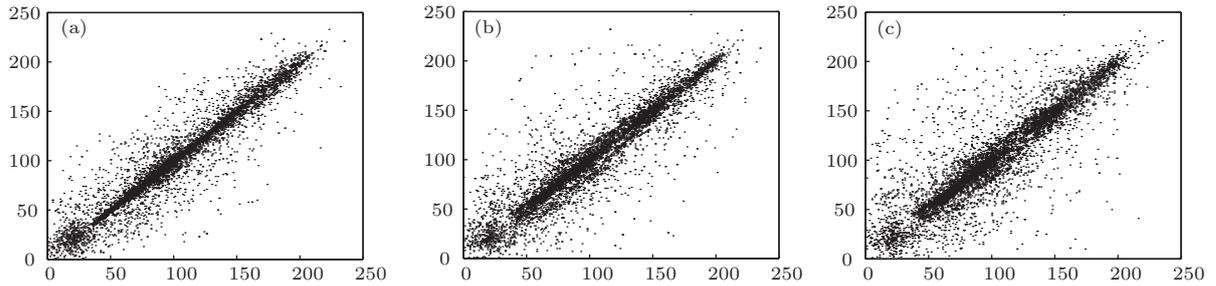


图9 原始图像相邻像素分布 (a) 垂直方向; (b) 水平方向; (c) 对角方向

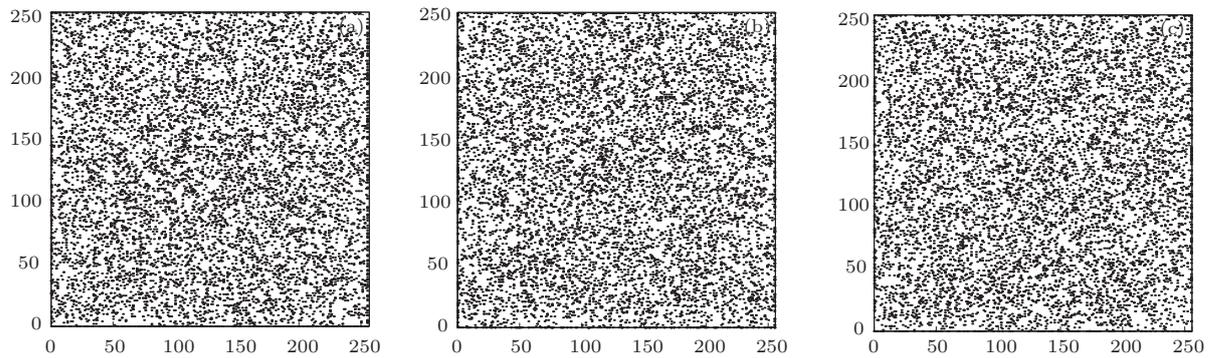


图10 新系统加密图像相邻像素分布 (a) 垂直方向; (b) 水平方向; (c) 对角方向

通过分析加密后的二维直方图熵和相关系数, 可以看出加密后图像相邻像素空间分布呈均匀状态, 表明相邻像素具有良好的随机特性. 对比表 5

中的数值可以看出, 五个系统混沌加密结果的熵值非常相似, 但是利用新系统进行混沌加密的相关性更小, 图像加密效果更好.

表5 加密后图像的相关系数和二维直方熵

加密系统	四个方向熵值	四个方向相关性
原系统	5.540308, 5.540067, 5.541347, 5.541022	-0.001134, 0.000565, -0.000065, -0.000111
Bao 系统	5.540789, 5.541111, 5.539764, 5.541319	0.000420, -0.000146, -0.000510, -0.000044
Tee 系统	5.541626, 5.541097, 5.539974, 5.541349	0.000215, -0.000015, -0.000343, 0.000630
Y 系统	5.539888, 5.538958, 5.539702, 5.540765	-0.000472, -0.000591, 0.000308, -0.000375
新系统	5.540321, 5.540848, 5.540164, 5.540501	0.000172, 0.000096, -0.000381, 0.000016

7 差分攻击

像素数变化率 R_{NPC} 和归一化平均变化强度 I_{UAC} 是衡量图像加密算法抵抗差分攻击的重要指标^[36]. R_{NPC} 和 I_{UAC} 分别表示随机地改变原始图像的某个像素值以后, 加密图像像素值发生改变的数目所占的比例以及变化程度. 若图像的某个像素值的改变可以很大程度地改变加密图像, 则说明该算法具有较强的抵抗差分攻击能力.

假设图像 C 和 C' 是两幅图像仅有一个像素之差的图像加密结果. 位置 (i, j) 处像素值分别记为

$C(i, j)$ 和 $C'(i, j)$. 像素数变化率和归一化平均变化强度指标分别描述为

$$R_{NPC} = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} D(i, j) \times 100\%, \quad (19)$$

$$I_{UAC} = \frac{1}{M \times N} \left(\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{C(i, j) - C'(i, j)}{255} \right) \times 100\%, \quad (20)$$

其中

$$D(i, j) = \begin{cases} 1, & C(i, j) \neq C'(i, j), \\ 0, & C(i, j) = C'(i, j). \end{cases}$$

将原始灰度 Lena 图像 (1, 23) 处的像素值由 148 改变为 149, 其改变前后两图像采用不同混沌系统加密结果所对应的 R_{NPC} 和 I_{UAC} 指标如表 6 所示.

表6 加密图像的 R_{NPC} 和 I_{UAC} 指标值

加密系统	$R_{NPC}/\%$	$I_{UAC}/\%$
原系统	70.63	11.67
Bao 系统	91.51	14.31
Tee 系统	95.93	17.47
Y 系统	79.33	6.33
新系统	96.59	23.91

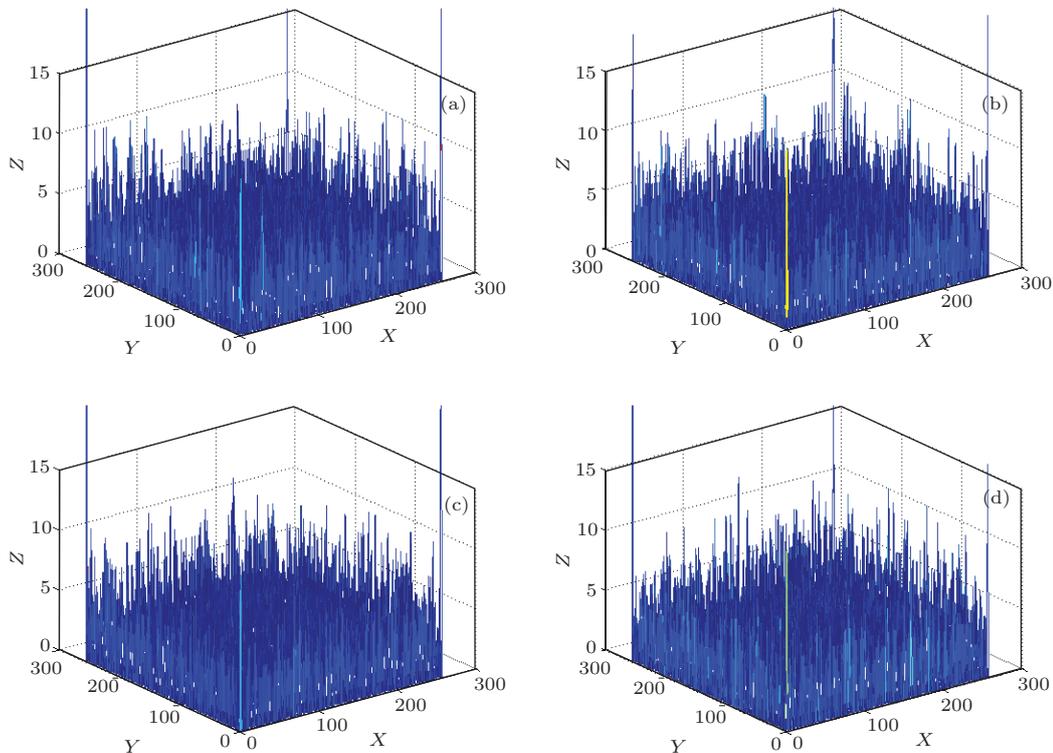


图11 利用新系统加密的二维直方图 (a) 0° 方向; (b) 45° 方向; (c) 90° 方向; (d) 135° 方向

通过比较,可以看出原始图像的稍微变化会引起密文图像的明显变化,且利用新系统加密所对应的 R_{NPC} 和 I_{UAC} 值更大,能够有效地抵御差分攻击,表明新系统在图像加密中具有更大的优势.

8 密钥敏感性测试

密钥敏感性是密码学的基本特性之一^[37],好的密码算法对密钥必须非常敏感.为了测试算法对密钥的敏感性,在利用新系统进行图像加密时,采用初始参数 $f_0 = (1, 1, 1)$ 生成的混沌密钥序列进行加密,然后采用有细微变化的初始参数 $f_0 = (1, 1.0000001, 1)$ 生成的混沌密钥序列去解密.图12分别给出了初始图像和该错误密钥的解密图像,可以看出,解密密钥稍有误差,解密图像与原始图像就截然不同,由此可见算法对解密密钥非常敏感.



图12 密钥敏感性测试 (a) 原始图像; (b) 错误密钥解密图像

9 结论

本文回顾了Lorenz系统的发展历程,分析了典型改进的Lorenz系统的构造方法,提出了一个新的改进的Lorenz混沌系统.通过对比五个不同改进的Lorenz系统的耗散性、对称性、平衡点稳定性、Lyapunov指数和维数等动力学特性,表明本文建议的新系统是一个高效的Lorenz混沌系统,且具有相对最大的正Lyapunov指数和维数,进一步拓展了广义Lorenz系统族,有利于推动现有Lorenz系统的发展.通过对比不同系统产生混沌序列的相关性和复杂度,表明新系统所产生的混沌序列具有良好的随机特性.利用不同系统产生的混沌序列对灰度图像加密,分析加密结果的相关性、共生矩阵熵、抗差分攻击和密钥敏感性测试,表明了新系统在图像加密、保密通信等领域具有良好的潜在优势.

参考文献

- [1] Lorenz E N 1963 *J. Atmos. Sci.* **20** 113
- [2] Pareek N K, Patidar V, Sud K K 2006 *Image Vision Comput.* **24** 9
- [3] Rhouma R, Belghith S 2008 *Phys. Lett. A* **372** 38
- [4] Singh N, Sinha A 2009 *Opt. Commun.* **282** 6
- [5] Cui L, Ou Q L, Zhang H Q 2010 *Commun. Technol.* **5** 43 (in Chinese) [崔力, 欧青立, 张红强 2010 通信技术 **5** 43]
- [6] Chen G R, Ueta T 1999 *Int. J. Bifur. Chaos* **9** 1465
- [7] Lü J H, Chen G R 2002 *Int. J. Bifur. Chaos* **12** 659
- [8] Qi G Y, Chen G R, Du S Z 2005 *Physica A* **352** 295
- [9] Elwakil A S, Özoğuz S, Kennedy P M 2002 *IEEE Trans. Circ. Syst.* **49** 4
- [10] Panchev S, Spassova T, Vitanov N K 2007 *Chaos, Soliton. Fract.* **33** 5
- [11] Zhao Z Y, Shu Y L, Zhang W X <http://www.paper.edu.cn/>
- [12] Wang Z, Mao P W 2008 *J. Dyn. Contr.* **6** 16 (in Chinese) [王震, 毛鹏伟 2008 动力学与控制学报 **6** 16]
- [13] Zhang Z Z, Shan Z P, Liu Y M 2013 *Appl. Math. Mech.* **34** 12 (in Chinese) [张转周, 陕振沛, 刘衍民 2013 应用数学和力学 **34** 12]
- [14] Huang G Q, Zhou Y Z 2013 *J. Inform. Comput. Sci.* **10** 4763
- [15] El-Sayed A M A, Salman S M 2013 *Electron. J. Math. Anal. Appl.* **1** 2
- [16] Tee L S, Salleh Z 2013 *J. Math.* **2013** 820946
- [17] Li C B, Wang H K, Huang X M 2009 *Microcomput. Inform.* **25** 8 (in Chinese) [李春彪, 王翰康, 黄新民 2009 微计算机信息 **25** 8]
- [18] Pan S Q, Liu Y J, Zhu C X 2013 *Comput. Engin. Appl.* **49** 7 (in Chinese) [庞寿全, 刘永建, 朱从旭 2013 计算机工程与应用 **49** 7]
- [19] Celikovskiy S, Chen G 2002 *Int. J. Bifur. Chaos* **12** 8
- [20] Sun K H, Sprott J C 2009 *Int. J. Bifur. Chaos* **19** 4
- [21] Bao B C 2013 *An Introduction to Chaotic Circuits* (Beijing: Science Press) p41 (in Chinese) [包伯成 2013 混沌电路导论 (北京: 科学出版社) 第41页]
- [22] Bao B C, Liu Z, Xu J P 2009 *J. Systems Eng. Electron.* **20** 6
- [23] Yuan D 2009 *J. Anyang Teach. Coll.* **2** 26 (in Chinese) [袁地 2009 安阳师范学院学报 **2** 26]
- [24] Luo X W, Wang C H, Wan Zhao 2014 *Nonlinear Anal. Model. Control* **19** 2
- [25] Li C G, Chen G R 2005 *Chaos, Soliton. Fract.* **5** 23
- [26] Liu Y J 2010 *Ph. D. Dissertation* (Guangzhou: South China University of Technology) (in Chinese) [刘永建 2010 博士学位论文 (广州: 华南理工大学)]
- [27] Grassberger P, Procaccia I 1983 *Physica D* **9** 189
- [28] Ramasubramanian K, Sriram M S 2000 *Physica D* **139** 72
- [29] Han M, Wei R 2010 *Syst. Eng. Electron.* **32** 11 (in Chinese) [韩敏, 魏茹 2010 系统工程与电子技术 **32** 11]
- [30] Guo J B, Xu X Z, Shi Q H, Hu T H 2013 *Acta Phys. Sin.* **62** 110508 (in Chinese) [郭静波, 徐新智, 史启航, 胡铁华 2013 物理学报 **62** 110508]

- [31] Wang Y X, Weng Y F, Zheng D L 2006 *J. Beijing Technol. Bus. Univ. (Nat. Sci. Ed.)* **24** 2 (in Chinese) [王云雄, 翁贻方, 郑德玲 2006 北京工商大学学报 (自然科学版) **24** 2]
- [32] Chen X J, Li Z, Bai B M, Pan W, Chen Q H 2011 *J. Electron. Inform. Technol.* **33** 5 (in Chinese) [陈小军, 李赞, 白宝明, 潘玮, 陈清华 2011 电子与信息学报 **33** 5]
- [33] Cao G H, Hu K 2013 *J. Beijing Univ. Aeron. Astron.* **39** 1 (in Chinese) [曹光辉, 胡凯 2013 北京航空航天大学学报 **39** 1]
- [34] Zhu C X, Sun K H 2012 *Acta Phys. Sin.* **61** 120503 (in Chinese) [朱从旭, 孙克辉 2012 物理学报 **61** 120503]
- [35] Li H N, Guo C F 2012 *J. Data Acquisi. Process.* **27** 1 (in Chinese) [李慧娜, 郭超峰 2012 数据采集与处理 **27** 1]
- [36] Wang J, Jiang G P 2011 *Acta Phys. Sin.* **60** 060503 (in Chinese) [王静, 蒋国平 2011 物理学报 **60** 060503]
- [37] Wang X Y, Xie Y X 2011 *Chin. Phys. B* **20** 8

An improved high performance Lorenz system and its application*

Guan Guo-Rong^{1)†} Wu Cheng-Mao¹⁾ Jia Qian²⁾

1) (School of Electronic Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710121 China)

2) (Shaanxi Lingyun Electronics Group Co., Ltd Design Institute, Baoji 721006 China)

(Received 3 June 2014; revised manuscript received 21 August 2014)

Abstract

Lorenz system is one of the most typical chaotic system models, and it has been well studied and widely applied. In order to obtain more complex structure and dynamic behavior of chaotic attractor for Lorenz system, improving the Lorenz system has become one of the important tasks in chaotic dynamical system. Therefore, an improved Lorenz system with complex dynamic behavior is proposed and used to protect image information security. Based on the existing various improvement Lorenz systems, firstly, a new Lorenz chaotic system is constructed by increasing the control parameters and modifying nonlinear expression in the existing Lorenz chaotic system; secondly, the mathematical properties of dissipation, symmetry, and stability in the proposed Lorenz system, which are similar to those in the existing Lorenz system, Bao system, Tee system and Y system, are investigated by modern differential dynamical system, and the experimental results of Lyapunov index and random sequence correlation of five different Lorenz systems show that the proposed Lorenz system has a more complex structure and chaotic dynamic behavior; finally, the discrete pseudo random sequences generated by five different Lorenz chaotic systems are used for scrambling the pixel position and diffusing the pixel value to protect image information security. The analyses of correlation and statistic histogram entropy of adjacent pixels, anti-differential attack and key sensitivity of the encrypted image, indicate that the improved Lorenz system proposed in this paper has much better potential advantages than other existing improved Lorenz system in image encryption application.

Keywords: Lorenz system, Lyapunov index, image encryption, correlation analysis

PACS: 05.45.-a, 02.30.Jr, 05.10.-a, 05.45.Tp

DOI: 10.7498/aps.64.020501

* Project supported by the National Natural Science Foundation of China (Grant No. 61136002), the Natural Science Foundation of Shaanxi Province, China (Grant Nos. 2014JM8331, 2014JQ5183, 2014JM8307), and the Scientific Research Project of the Education Department of Shaanxi Province, China (Grant No. 2013JK1129).

† Corresponding author. E-mail: guanguorong@126.com